REMARKS

Claims 1-21 are presented for further examination. Claims 1, 9, 10, 13, 16, and 19 have been amended.

In the final Office Action mailed March 23, 2009, the Examiner maintained the rejection of claims 1-21 under 35 U.S.C. § 103(a) as obvious over previously-cited Chaney in combination with previously-cited Mills.

Applicants respectfully request reconsideration and further examination of the claims.

Claim Rejection

The primary reference relied upon by the Examiner, Chaney, describes the use of a common key to decrypt broadcast data. However, Chaney does not disclose or teach the use of a broadcasted common key to decrypt the control signals (ECM data). The "common key" of Chaney is provided on a smart card (see column 11, lines 15-22). Such smart cards are removable devices that plug into a set top box or other similar decoder and, hence, are susceptible to tampering because they can be easily accessed.

The Examiner further relies on Mills, which discloses a common key provided via broadcast (column 11, lines 32-35). The Examiner asserts that combining Chaney and Mills produces a similar integrated circuit to that of claim 1. However, neither of the cited documents mentions the specific routing as required by claim 1. It appears the Examiner may be using hindsight to infer how one of skill would route the common keys.

Applicants previously argued that Chaney discloses common keys provided directly from a smart card and not via broadcast. The Examiner responded that claim 1 did not require the system to receive common keys by broadcast. Applicants have amended all of the independent claims to indicate that the common keys are received by broadcast and, in addition, they are received in encrypted form.

The Examiner maintains that Chaney discloses a common key store in an integrated circuit. While Chaney does disclose a RAM (426) that is used to store a key, that key is generated on the smart card and is used to descramble particular types of data (see column 6, lines 55-67). Presumably this could include a common key used to descramble control signals.

As such, the method and device of Chaney is susceptible to the tampering described in the background portion of the present application.

The Examiner maintains that Mills discloses a common key encrypted according to a secret key stored on the smart card. At column 11, lines 32-41, Mills states that EMMs, which may contain an encrypted service key used to decrypt ECMs, are stored in a DRAM 40 for transmission (over an insecure external interface) to the smart card and subsequent decryption. The secret key is used to decrypt the encrypted service key. There is no teaching or suggestion in Mills of subsequent storage of the decrypted service key.

It appears the Examiner is saying that:

(1) Mills teaches use of an encrypted common key (provided over a broadcast), and the use of a secret key to decrypt the common key;

(2) Chaney discloses a common key store; and

(3) It would be obvious to combine Mills with Chaney to produce a monolithic circuit that stores decrypted common keys.

However, it is not evident to one of ordinary skill that such a system would be arranged such that the only route to placing a common key in the common key store is to receive by broadcast the common key in encrypted form for decryption in accordance with a secret key. Moreover, Chaney shows multiple buses connected to the RAM 426, which functions as a key store (see Figure 4), neither Chaney nor Mills teach or suggest storing the decrypted common key after receipt of the encrypted common mode key by broadcast.

Chaney does not disclose the particular claimed routing system for common keys because Chaney's RAM 426 is not dedicated to storing common keys. It also stores other data, such as entitlements, etc. and is not a dedicated common key store. In addition, the specific routing system recited in the claims means that it is not possible to make use of the common keys without knowing the secret key because, before use, the common key is routed through the (second) decryption circuit. Applicants further note that nowhere in the cited art is there any teaching that an encrypted key must be decrypted before it is stored. Moreover, it is arguably counterintuitive, since one may suppose that it is more secure to store a common key in encrypted form.

In addition, given that the RAM 426 in Chaney is connected to a CPU, access to the RAM 426 must be software based, rather than being hardwired. Thus, it could be possible in Chaney to "spoof" the CPU and gain access to the keys stored in the RAM.

The main security provided by the current claimed embodiments comes from the fact that a monolithic circuit, preferably located in the set top box, is used to perform all decryption, thus eliminating vulnerable interfaces, and also that the manner in which the broadcast keys are routed is handled in hardware by a hardwired path. The references cited and relied upon by the Examiner fail to teach or suggest this feature.

A key concept in the present claimed embodiments is to provide set top boxes with built-in monolithic circuits that receive broadcast signals, including encrypted audio/video data, encrypted control signals (instructions that tell the device how to decrypt the audio/video data), and encrypted common keys used to decrypt the control signals. Thus, the claimed embodiments eliminate the use of replaceable smart cards and receive everything via broadcast except for a single, user-specific, secret key stored within the set top box monolithic circuit.

Turning to the claims, claim 1 has been amended to recite, *inter alia*, an input interface for receipt of received encrypted broadcast signals, a broadcast encrypted common key, and control data. Claim 1 also recites, *inter alia*, decrypting control signals in a first decryption circuit in accordance with a decrypted common key from a dedicated common key store in the integrated circuit. Claim 1 in addition recites that the circuit is arranged such that the only route to placing a decrypted common key in the common key store is to receive by broadcast the common key in encrypted form for decryption in accordance with the secret key, and to provide the common key to the common key store over an internal bus.

The primary reference relied upon by the Examiner, Chaney, teaches the use of a smart card. The Examiner relies upon the secondary reference, Mills, to teach receiving a common key by broadcast. However, neither Chaney nor Mills, taken alone or in any combination thereof, teach or suggest first decrypting the common key and then storing the decrypted common key in a dedicated common key store. It would be intuitive, rather, to store the common key in encrypted form and then later decrypt it just prior to use. There is no teaching or suggestion of storing the decrypted common key in a dedicated common key store as

recited in claim 1. Thus, claim 1 makes it clear that the encrypted common key is received by broadcast, and then after decryption the common key is stored in a dedicated common key store. Neither Chaney nor Mills teach or suggest these features, taken alone or in any combination therewith. Applicants respectfully submit that claim 1 and corresponding dependent claims 2-8 are allowable over the combination of Chaney and Mills.

Independent claim 9 is directed to a system that recites, *inter alia*, the semiconductor integrated circuit of independent claim 1. Applicants respectfully submit that independent claim 9 is allowable for the features recited therein as well as for the reasons why claim 1 is allowable.

Independent claim 10 is directed to a set top decoder device for decryption of the broadcast signals, including a monolithic device located in the set top box. The specification at page 7, lines 25-26 provide support for the monolithic device being located in the set top box. In contrast, Chaney clearly teaches the use of a smart card that is not located in the monolithic device. Moreover, the combination of Chaney and Mills fails to teach a common key store in the monolithic device and configured to receive a common key, a secret key store in the monolithic device configured to store a secret key. In view of the foregoing, applicants respectfully submit that claim 10 and corresponding dependent claims 11 and 12 are allowable over the combination of Chaney and Mills.

Independent claim 13 is directed to a method of decrypting encrypted broadcast signals that includes receiving encrypted broadcast signals, encrypted broadcast control signals, and encrypted broadcast common key signals at an input interface. As previously argued in the prior amendment and reiterated herein, the use of broadcasted common key signals that are encrypted for later decryption and storage in a common key store in a semiconductor integrated circuit that is arranged such that the only route to placing a common key in the common key store is to receive the common key by broadcast in encrypted form for decryption and then storing in the common key store in decrypted form. Applicants respectfully submit that claim 13 and corresponding dependent claims 14 and 15 are allowable over the combination of Chaney and Mills.

Independent claim 16 is also directed to a method for broadcasting signals to a plurality of subscribers and includes, *inter alia*, broadcasting encrypted control words, encrypted common key, and encrypted broadcast signals to the plurality of subscribers and receiving the same in a decryption unit where the common key is first decrypted and then stored in a dedicated common key store. Applicants respectfully submit that claim 16 and dependent claims 17 and 18 are allowable over the combination of Chaney and Mills for the reasons discussed above with respect to the prior independent claims.

Independent claim 19 is directed to a system for broadcasting signals to a plurality of subscribers that contains similar limitations to those of the prior independent claims. Applicants respectfully submit that claim 19 and corresponding dependent claims 20 and 21 are allowable over the combination of Chaney and Mills for the reasons discussed above with respect to the prior claims.

In view of the foregoing, applicants respectfully submit that the claims remaining in this application are in condition for allowance. In the event the Examiner disagrees or finds minor informalities that can be resolved by telephone conference, the Examiner is urged to contact the undersigned by telephone at (206) 622-4900 in order to expeditiously resolve prosecution of this application. Consequently, early and favorable action allowing these claims and passing this case to issuance is respectfully solicited.

The Director is authorized to charge any additional fees due by way of this Amendment, or credit any overpayment, to our Deposit Account No. 19-1090.

Respectfully submitted,

SEED Intellectual Property Law Group PLLC

/E. Russell Tarleton/
E. Russell Tarleton
Registration No. 31,800

ERT:jl

701 Fifth Avenue, Suite 5400
Seattle, Washington 98104
Phone: (206) 622-4900 | Fax: (206) 682-6031
1414308_1.DOC